FORTINET
High Performance Network Security

FortiGate-5001E Security System Guide

01-560-410512-201700905

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, September 05, 2017

FortiGate-5001E Security System Guide

01-560-410512-201700905

TABLE OF CONTENTS

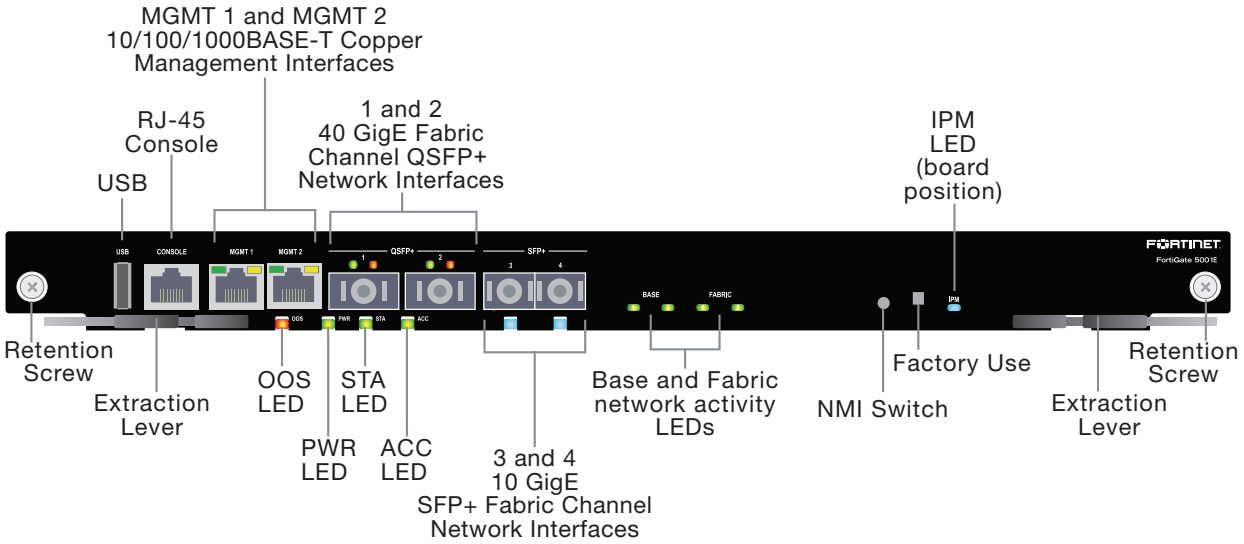
FortiGate-5001E and FortiGate-5001E1 security system

The FortiGate-5001E security system is a high-performance Advanced Telecommunications Computing Architecture (ATCA) compliant FortiGate security system that can be installed in any ATCA chassis that can provide sufficient power and cooling. The FortiGate-5001E1 security system adds an internal 480 GByte SSD log disk. In all other ways the FortiGate-5001E and the FortiGate-5001E1 are identical.

The FortiGate-5001E is compatible with Fortinet's FortiGate-5144C chassis. See the FortiGate-5000 Compatibility Guide for up-to-date information about FortiGate-5001E compatability.

The FortiGate-5001E security system contains two front panel 40GigE QSFP+ fabric channel interfaces, two front panel 10GigE SFP+ fabric channel interfaces, two base backplane 1Gbps base channel interfaces, and two fabric backplane 40Gbps interfaces. The front panel SFP+ interfaces can also operate as Gigabit Ethernet interfaces using SFP transceivers. Use the front panel interfaces for connections to your networks and the backplane interfaces for communication across the ATCA chassis backplane. The FortiGate-5001E also includes two front panel 10/100/1000BASE-T out of band management Ethernet interfaces, one RJ45 front panel serial console port, and one front panel USB port.

FortiGate-5001E front panel



The FortiGate-5001E front panel 40GigE, 10GigE interfaces and fabric backplane interfaces also provide NP6-accelerated network processing for eligible traffic passing through these interfaces. All data traffic can also be accelerated by CP9 processors.

You can also configure two or more FortiGate-5001Es to create a high availability (HA) cluster using the base or fabric backplane interfaces for HA heartbeat communication through the chassis backplane, leaving front panel interfaces available for network connections.

In most cases the base backplane interfaces are used for HA heartbeat communication and the fabric backplane interfaces are used for data communication.

The FortiGate-5001E also supports high-end FortiGate features including 802.1Q VLANs, multiple virtual domains, 802.3ad aggregate interfaces, and FortiOS Carrier.

The FortiGate-5001E includes the following features:

- Two front panel 40GigE QSFP+ fabric channel (port1 and port2) accelerated by NP6 network processors. Using 40GBASE-SR10 multimode QSFP+ transceivers, port1 and port2 can also be split into four 10GBASE-SR interfaces using the `config system global set split-port` command.
- Two front panel 10GigE SFP+ fabric channel interfaces (port3 and port4) also accelerated by NP6 network processors. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers.
- Two front panel 10/100/10000BASE-T out of band management Ethernet interfaces (mgmt1 and mgmt2).
- Two base backplane 1Gbps interfaces (base1 and base2) for HA heartbeat communications across the FortiGate-5000 chassis base backplane.
- Two fabric backplane 40Gbps interfaces (fabric1 and fabric2) for data communications across the FortiGate-5000 chassis fabric backplane.
- Two NP6 network processors that accelerate traffic on the interfaces port1 - port4, fabirc1, and fabric2.
- Four CP9 content processors that accelerate IPS, DLP, SSL VPN, key exchange, and IPsec VPN.
- The FortiGate-5001E1 includes a 480 GB SSD for storing log messages, DLP archives, historic reports, IPS packet archiving, file quarantine, WAN Optimization byte caching and web caching.
- One RJ-45 RS-232 serial console connection.
- 1 USB connector.
- NMI switch for troubleshooting as recommended by Fortinet Support.
- Mounting hardware.
- LED status indicators.

Physical Description

Dimensions	1.2 x 11.34 x 14 in. (3.1 x 28.8 x 35.1 cm) (Height x Width x Depth)
Weight	8.2 lb. (3.7 kg)
Operating Temperature	23 to 131°F (-5 to 55°C)
Storage Temperature	-40 to 158°F (-40 to 70°C)
Relative Humidity	5 to 90% (Non-condensing)
Power consumption Maximum	278 W
Average Power Consumption	250 W
Max Current	5.9 A
Heat Dissipation	948.6 BTU/h

Front panel components

From the FortiGate-5001E front panel you can view the status of the front panel LEDs to verify that the board is functioning normally. You also connect the FortiGate-5001E to your 40-gigabit network using the front panel QSFP+ connectors and to your 10-gigabit network using the front panel SFP+ or SFP connectors. The front panel also includes two Ethernet management interfaces, an RJ-45 console port for connecting to the FortiOS CLI and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

LEDs

Ports 1 and 2 can operate in 40-gigabit mode or 4 x 10-gigabit mode. The LEDs function differently in each mode.

System LEDs

LED	State	Description
OOS (Out of Service)	Off	Normal operation.
	Red	A fault condition exists and the FortiGate-5001E is out of service (OOS). This LED may also flash very briefly during normal startup.
PWR (Power)	Off	The main power is off. The standby power for IPMC circuits maybe powered on in this state.
	Green	The FortiGate-5001E is powered on.
STA (Status)	Off	The FortiGate-5001E is operating normally.
	Flashing Green	The FortiGate-5001E is starting up. If this LED is flashing at any time other than system startup, a fault condition may exist.
ACC (Disk activity)	Off or Flashing green	The ACC LED flashes green when the FortiGate-5001E accesses the flash disk. The flash disk stores the current firmware build and configuration files. The system accesses the flash disk when starting up, during a firmware upgrade, or when an administrator is using the CLI or GUI to change the FortiGate-5001E configuration. Under normal operating conditions this LED flashes occasionally, but is mostly off. Also flashes green when the FortiGate-5001E1 reads or writes the 480 GB SSD.

LED	State	Description
IPM (Hot Swap)	Off	Normal Operation. The FortiGate-5001E is in contact with the chassis backplane.
	Flashing Blue	The FortiGate-5001E is changing from hot swap to running mode or from running mode to hot swap. This happens when the FortiGate-5001E is starting up or shutting down.
	Blue	The FortiGate-5001E is ready to be hot-swapped (removed from the chassis). If the IPM light is blue and no other LEDs are lit the FortiGate-5001E has lost power.

BASE and FABRIC network activity LEDs

LED	State	Description
BASE (left base1, right base2)	Green	Base backplane interfaces are connected at 1 Gbps.
	Flashing Green	Network activity.
	Off	No link.
FABRIC (left fabric1, right fabric2)	Green	Fabric backplane interface is connected at 40 Gbps.
	Flashing Green	Network activity.
	Off	No link.

QSFP+ network activity LEDs (port1 and port2) (40G or 4 x 10G)

Left LED	Right LED	Description
Green	Off	Connected at 40Gbps.
Flashing Green	Amber	Connected at 10Gbps.
Flashing Green	Flashing Amber	Connected at 10 Gbps (less than 4 channels).
Off	Off	No link established.

SFP+ network activity LEDs (port3 and port4) (10G)

LED	State	Description
Link/ACT	Green	SFP+ interface connected at 10Gbps.
	Flashing Green	Network activity.
	Off	No link.

RJ45 management interface LEDs (MGMT1 and MGMT2)

LED	State	Description
Link/ACT (left)	Green	Link up.
	Flashing Green	Network activity.
	Off	No link.
Speed (right)	Green	Management interface connected at 1 Gbps.
	Amber	Management interface connected at 100 Mbps.
	Off	No link, or management interface connected at 10 Mbps.

Front panel connectors

Connector	Type	Speed	Protocol	Description
CONSOLE	RJ-45	9600 bps 8/N/1	RS-232 serial	Serial connection to the command line interface.
1 and 2	QSFP+ (40 gigabit) SFP+ (10 gigabit)	40-gigabit full 4x10-gigabit full	Ethernet	40-gigabit QSFP+ connection to 40GigE networks or 4x10GigE SFP+ connection to 10GigE networks. Quad small form-factor pluggable transceiver.
3 and 4	SFP+ (10 gigabit) SFP (1 gigabit)	10-gigabit full 1-gigabit auto 1-gigabit full	Ethernet	10GigE SFP+ connection to 10GigE networks or 1GigE SFP connection to 1GigE networks. Small form-factor pluggable transceiver.

Connector	Type	Speed	Protocol	Description
MGMT1 and MGMT2	RJ-45	10/100/1000 Base-T	Ethernet	Copper 1GigE connection to 10/100/1000Base-T copper networks for management or system administration.
USB	USB			USB key for firmware updates and configuration backup.

NMI switch

When working with Fortinet Support to troubleshoot problems with the FortiGate-5001E you can use the front panel non-maskable interrupt (NMI) switch to assist with troubleshooting. Pressing this switch causes the software to dump registers/backtraces to the console. After the data is dumped the FortiGate-5001E reboots. While rebooting, traffic is temporarily blocked. The FortiGate-5001E should restart normally and traffic can resume once its up and running.

Base backplane communication

The FortiGate-5001E base backplane 1-gigabit interfaces (base1 and base2) are typically used for HA heartbeat or other management base backplane communication. You can also configure FortiGate-5001Es to use the base backplane interfaces for data communication. To support base backplane communications your FortiGate-series chassis must include one or more FortiSwitch or FortiController or other 1-gigabit base backplane switches installed in the chassis in hub/switch slots 1 and 2.

See the FortiGate-5000 Compatibility Guide for up-to-date information about FortiGate-5000 components that are compatible with the FortiGate-5001E.

Fabric backplane communication

The FortiGate-5001E fabric backplane interfaces (fabric1 and fabric2) are typically used for fabric backplane data communication. These interfaces can operate as 40-gigabit or 10-gigabit interfaces

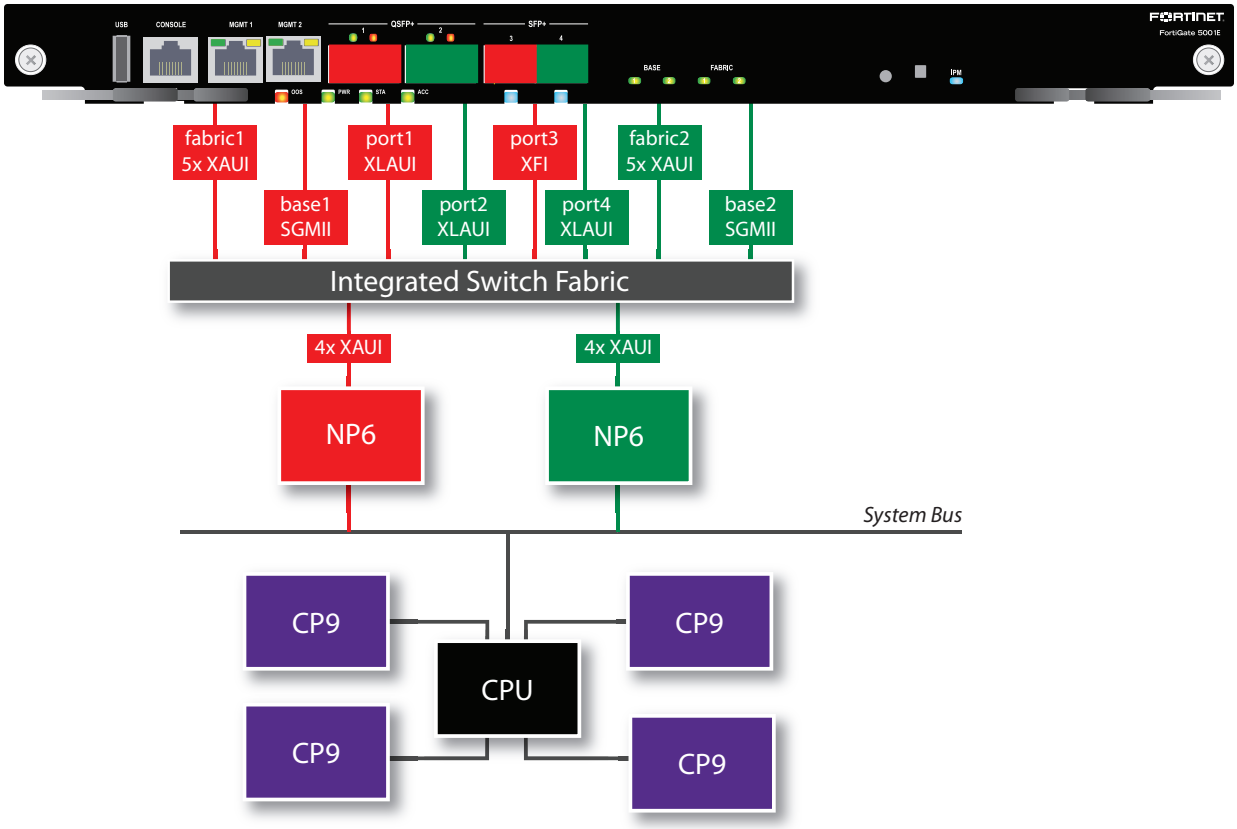
To support 40-gigabit fabric backplane communications your FortiGate-5000 series chassis must include one or more FortiControllers or other 40-gigabit fabric backplane switches installed in the chassis in fabric slots 1 and 2.

To support 10-gigabit fabric backplane communications your FortiGate-5000 series chassis must include one or more FortiSwitches or FortiControllers or other 10-gigabit fabric backplane switches installed in the chassis in hub/switch slots 1 and 2.

See the FortiGate-5000 Compatibility Guide for up-to-date information about FortiGate-5000 components that are compatible with the FortiGate-5001E.

Accelerated packet forwarding and policy enforcement (NP6 network processors)

The FortiGate-5001E includes two NP6 processors and an integrated switch fabric (ISF) that provides fastpath acceleration by offloading communication sessions from the FortiGate CPU. All traffic from the front panel and backplane interfaces can be accelerated. The result is enhanced network performance provided by the NP6 processor plus the network processing load is removed from the CPU. The NP6 processor can also handle some CPU intensive tasks, like IPsec VPN encryption/decryption. Because of the integrated switch fabric, all sessions are fast-pathed and accelerated.



Accelerated IPS, SSL VPN, and IPsec VPN (CP9 content processors)

The FortiGate-5001E includes four CP9 processors that provide the following performance enhancements:

- Flow-based inspection (IPS, application control etc.) pattern matching acceleration with over 10Gbps throughput
  - IPS pre-scan
  - IPS signature correlation
  - Full match processors
- High performance VPN bulk data engine

    - IPsec and SSL/TLS protocol processor
    - DES/3DES/AES128/192/256 in accordance with FIPS46-3/FIPS81/FIPS197
    - MD5/SHA-1/SHA256/384/512-96/128/192/256 with RFC1321 and FIPS180
    - HMAC in accordance with RFC2104/2403/2404 and FIPS198
    - ESN mode
    - GCM support for NSA "Suite B" (RFC6379/RFC6460) including GCM-128/256; GMAC-128/256
- Key Exchange Processor that supports high performance IKE and RSA computation
    - Public key exponentiation engine with hardware CRT support
    - Primary checking for RSA key generation
    - Handshake accelerator with automatic key material generation
    - True Random Number generator
    - Elliptic Curve support for NSA "Suite B"
    - Sub public key engine (PKCE) to support up to 4096 bit operation directly (4k for DH and 8k for RSA with CRT)
- DLP fingerprint support
    - TTTD (Two-Thresholds-Two-Divisors) content chunking
    - Two thresholds and two divisors are configurable

Splitting the FortiGate-5001E front panel port1 and port2 interfaces

You can use the following command to split the 40-gigabit front panel port1 interface into a 4 x 10-gigabit interface:

```
config system global
   set split-port port1
end
```

The FortiGate-5001E reboots and when it does you can see four new interfaces named port1/1, port1/2, port1/3, and port1/4.

Hardware installation

This chapter describes installing a FortiGate-5001E (sometimes just referred to as a "board") into a chassis. Before use, the FortiGate-5001E must be correctly inserted into an Advanced Telecommunications Computing Architecture (ATCA) chassis that can provide sufficient power and cooling.

Installing QSFP+ and SFP+ transceivers

You must install QSFP+ transceivers to connect the FortiGate-5001E front panel 1 and 2 interfaces to a 40Gbps network. The QSFP+ transceivers are inserted into cage sockets numbered 1 and 2 on the FortiGate-5001E front panel. You can install the QSFP+ transceivers before or after inserting the FortiGate-5001E into a chassis.

You can split front panel interfaces 1 and 2 into four 10GBASE-SR interfaces by installing 40GBASE-SR10 multimode QSFP+ transceiver.

You must install SR SFP+ transceivers for normal operation of the FortiGate-5001E front panel 3 and 4 interfaces. The FortiGate-5001E ships with two SR SFP+ transceivers. You can also configure the 3 and 4 interfaces to operate at 1Gbps and install SFP transceivers. You can install the transceivers before or after inserting the FortiGate-5001E into a chassis.

You can install the following types of transceivers for connectors 3 and 4:

- SFP+ SR (10Gbps)
- SFP+ LR (10Gbps)
- SFP (1Gbps)

To install QSFP+, SFP+ or SFP transceivers

To complete this procedure, you need:

- A FortiGate-5001E
- QSFP+, SFP+ or SFP transceivers
- An electrostatic discharge (ESD) preventive wrist or ankle strap with connection cord

FortiGate-5001Es must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001Es at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001Es.

Handling the QSFP+, SFP+ and SFP transceivers by holding the release latch can damage the connector. Do not force transceivers into their cage slots. If the transceiver does not easily slide in and click into place, it may not be aligned correctly. If this happens, remove the transceiver, realign it and slide it in again.

1. Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.
2. Remove the caps from the cage sockets on the FortiGate-5001E front panel.

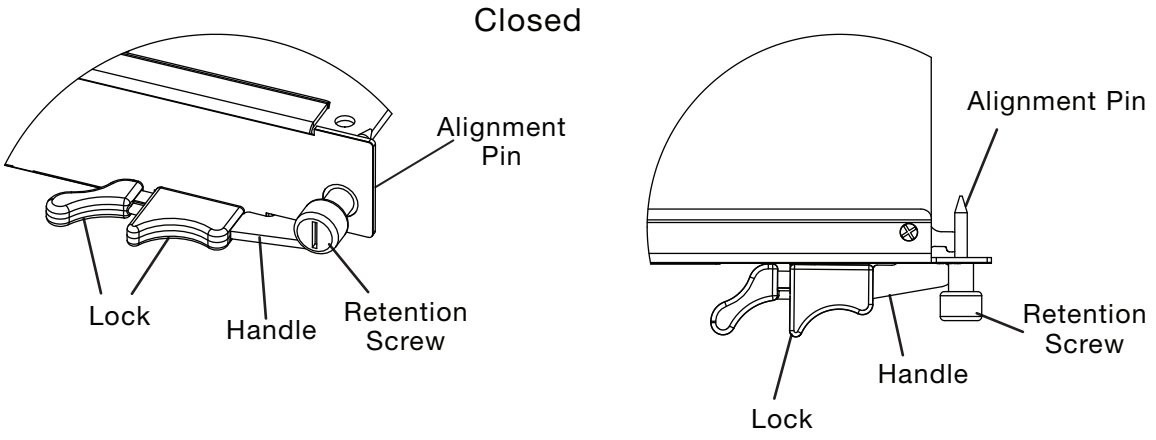
3. Hold the sides of the transceiver and slide it into the cage socket until it clicks into place.

FortiGate-5001E mounting components

To install a FortiGate-5001E you slide the board into a hub/switch slot in the front of an ATCA chassis (usually slot 3 plus) and then use the mounting components to lock the board into place in the slot. When locked into place and positioned correctly the board front panel is flush with the chassis front panel. The board is also connected to the chassis backplane.

FortiGate-5001Es are vertical when inserted into a FortiGate-5144C chassis, but you also often see the board on a horizontal surface or horizontally in an illustration. Because of this, the descriptions in this document refer to left (top) and right (bottom) mounting components.

To position the board correctly you must use the mounting components shown below for the right (bottom) of the FortiGate-5001E front panel. The mounting components on the left (top) of the front panel are the same but reversed. The FortiGate-5001E mounting components align the board in the chassis slot and are used to insert and eject the board from the slot.



The FortiGate-5001E handles align the board in the chassis slot and are used to insert and eject the board from the slot. The right (bottom) handle activates a microswitch that turns on or turns off power to the board. When the

right (bottom) handle is open the microswitch is off and the board cannot receive power. When the right (bottom) handle is fully closed the microswitch is on and if the board is fully inserted into a chassis slot the board can receive power.

Inserting a FortiGate-5001E board into a chassis

The FortiGate-5001E must be fully installed in a chassis slot (usually slot 3 plus), with the handles closed and locked and retention screws fully tightened for the FortiGate-5001E to receive power and operate normally. If the FortiGate-5001E is not receiving power, the HS LED glows solid blue and all other LEDs remain off.

It is important to carefully seat the FortiGate-5001E all the way into the chassis, to not use too much force on the handles, and to make sure that the handles are properly locked. Only then will the FortiGate-5001E power-on and start up correctly.

FortiGate-5001Es are hot swappable. The procedure for inserting a FortiGate-5001E into a chassis slot is the same whether or not the chassis is powered on.

To insert a FortiGate-5001E into a chassis slot

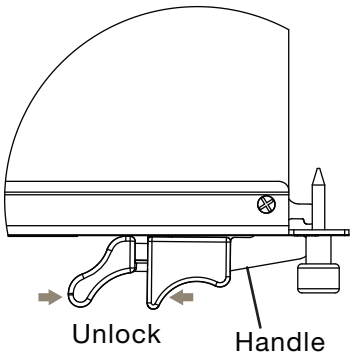
Do not carry the FortiGate-5001E by holding the handles or retention screws. When inserting or removing the FortiGate-5001E from a chassis slot, handle the board by the front panel. The handles are not designed for carrying the board. If the handles become bent or damaged the FortiGate-5001E may not align correctly in the chassis slot.

To complete this procedure, you need:

- A FortiGate-5001E
- An ATCA chassis with an empty hub/switch slot
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

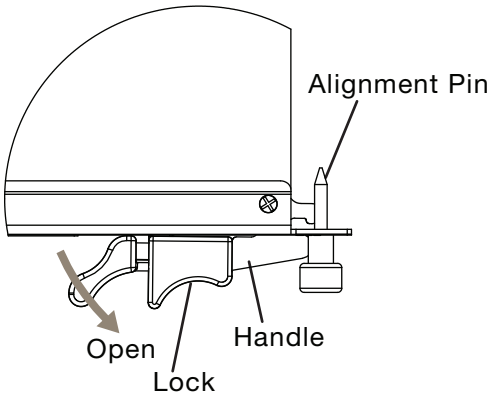
FortiGate-5001Es must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001Es at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001Es.

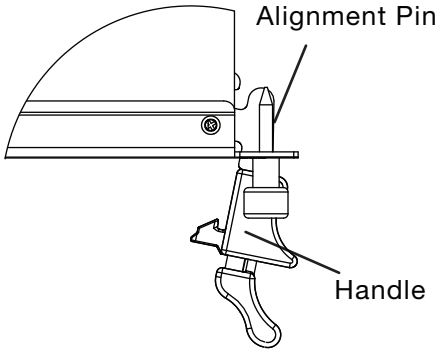
1. Attach the ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. If required, remove the protective metal frame that the FortiGate-5001E has been shipped in.
3. Insert the FortiGate-5001E into the empty slot in the chassis.
4. Unlock the handles by squeezing the handle locks.



5. Open the handles to their fully open positions.

To avoid damaging the lock, make sure you squeeze the handles fully to unlock them before opening. The handles should pop easily out of the board front panel

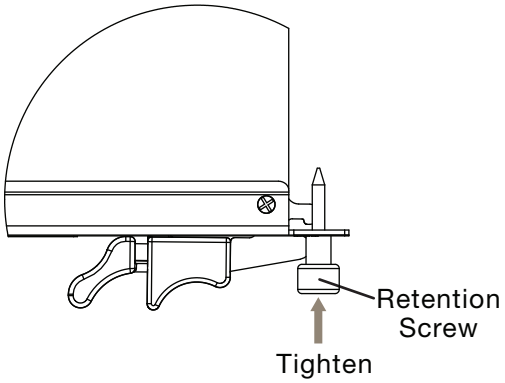




6. Carefully guide the FortiGate-5001E into the chassis using the rails in the slot.
   Insert the FortiGate-5001E by applying moderate force to the front faceplate (not the handles) to slide the board into the slot. The board should glide smoothly into the chassis slot. If you encounter any resistance while sliding the board in, the board could be aligned incorrectly. Pull the board back out and try inserting it again.
7. Slide the board in until the alignment pins are inserted half way into their sockets in the chassis.
8. Turn both handles to their fully-closed positions.
   The handles should hook into the sides of the chassis slot. Closing the handles draws the board into position in the chassis slot and into full contact with the chassis backplane. The board front panel should be in contact with the chassis front panel. When the handles are fully-closed they lock into place.

   As the right (bottom) handle closes the microswitch is turned on, supplying power to the board. If the chassis is powered on the HS LED starts flashing blue. If the board is aligned correctly, inserted all the way into the slot, and the right (bottom) handle is properly closed the HS LED flashes blue for a few seconds. At the same time the ACC LEDs turn green. After a few seconds the HS LED goes out and the FortiGate-5001E firmware starts up. If the board is operating correctly, the front panel LEDs are lit as described below.

   If the board has not been inserted properly the HS LED changes to solid blue and all other LEDS turn off. If this occurs, open the handles, slide the board part way out, and repeat the insertion process.
9. Once the board is inserted correctly, fully tighten the retention screws to lock the FortiGate-5001E into position in the chassis slot.



FortiGate-5001E normal operating LEDs

LED	State
OOS	Off
PWR	Green
STA	Off
ACC	Off (Or flashing green when the system accesses the FortiController-5903C flash disk.)
IPM	Off

Shutting down and Removing a FortiGate-5001E

To avoid potential hardware problems, always shut down the FortiGate-5001E operating system properly before removing the FortiGate-5001E from a chassis slot or before powering down the chassis.

The following procedure describes how to correctly use the FortiGate-5001E mounting components to remove a FortiGate-5001E from an ATCA chassis slot.

FortiGate-5001E are hot swappable. The procedure for removing a FortiGate-5001E from a chassis slot is the same whether or not the chassis is powered on.

To remove a FortiGate-5001E from a chassis slot

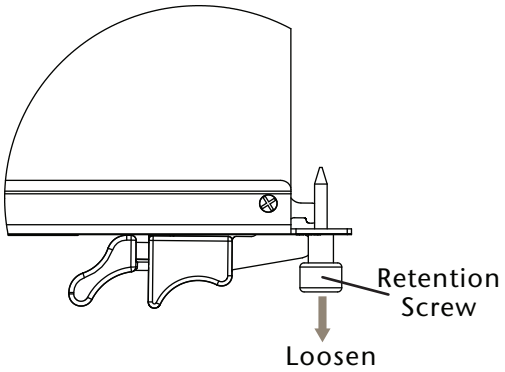
Do not carry the FortiGate-5001E by holding the handles or retention screws. When inserting or removing the FortiGate-5001E from a chassis slot, handle the board by the front panel. The handles are not designed for carrying the board. If the handles become bent or damaged theFortiGate-5001E may not align correctly in the chassis slot.

To complete this procedure, you need:

- An ATCA chassis with a FortiGate-5001E installed
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

FortiGate-5001Es must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001Es at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001Es.

1. Attach the ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Disconnect all cables from the FortiGate-5001E, including all network cables and the console cable.
3. Fully loosen the FortiGate-5001E retention screws.

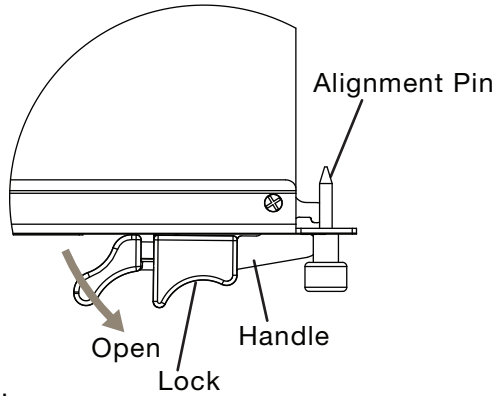


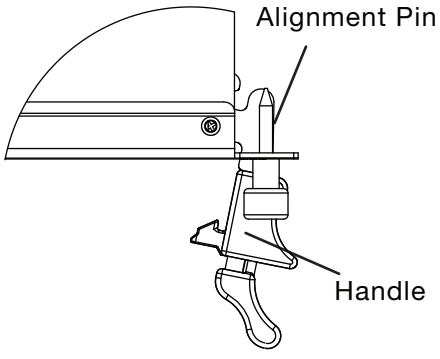
4. Unlock the handles by squeezing the handle locks.
5. Slowly open both handles a small amount (about 8 degrees) until the IPM LED flashes blue.
6. Keep the handles in this position until the IPM LED stops flashing and becomes solid blue.

Waiting for the IPM LED to change to solid blue makes sure that the board software shutdowns completely before disconnecting it from backplane power.

7. Open the handles to their fully open positions.
   Opening the handles turns off the microswitch, turns off all LEDs, and ejects the board from the chassis slot. You need to use moderate pressure on the handles to eject the board

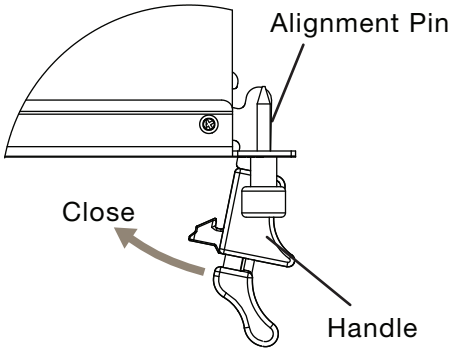
To avoid damaging the lock, make sure you squeeze the handles fully to unlock them before opening. The handles should pop easily out of the board front panel.

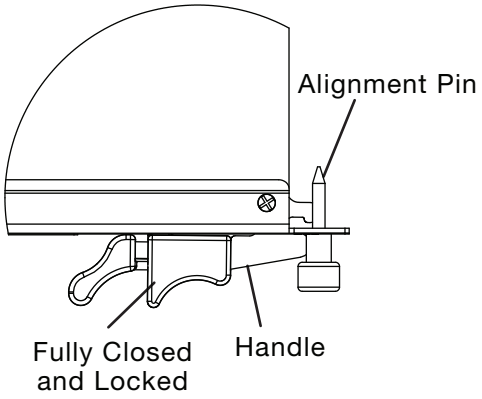




.

8. Pull the board about half way out.
9. Turn both handles to their fully-closed positions.
   When the handles are fully-closed they lock into place.





10. Carefully slide the board completely out of the slot.
11. Re-attach the protective metal frame if you are going ship the FortiGate-5001E or store it outside of a chassis.

Resetting a FortiGate-5001E

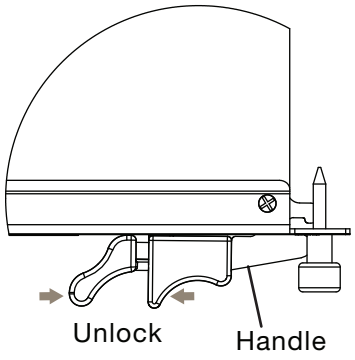
You can use the following procedure to reset a FortiGate-5001E without removing it from the chassis. You do not have to loosen the retention screws or adjust the position of the FortiGate-5001E to use this procedure.

To complete this procedure, you need:

- An ATCA chassis with a FortiGate-5001E installed
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

FortiGate-5001Es must be protected from static discharge and physical shock. Only handle or work with FortiGate-5001Es at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate-5001Es.

1. Attach the ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Unlock the right handle by squeezing the handle lock.



3. Pivot the right handle open.
   The handle can only pivot a short distance. Pivoting the right handle turns off the microswitch which powers down the board, turning off all LEDs except the IPM LED which turns on.
4. After 10 seconds snap the right handle back into place.
5. The board powers up, the LEDs light and in a few minutes the FortiGate-5001E operates normally.

Troubleshooting

This section describes some common troubleshooting topics:

FortiGate-5001E does not startup

Positioning of FortiGate-5001E handles and a few other causes may prevent a FortiGate-5001E from starting up correctly.

Chassis with a shelf manager: no communication with shelf manager

If the FortiGate-5001E is receiving power and the handles are fully closed and the FortiGate-5001E still does not start up, the problem could be that the FortiGate-5001E cannot communicate with the chassis shelf manager. This problem can only occur in an ATCA chassis that contains a shelf manager.

To correct this problem power down and then restart the chassis. If you are operating a FortiGate-5000 series chassis you can power down and then restart the chassis without removing FortiGate-5000 series components.

All chassis: handles not fully closed

If the handles are damaged or positioned incorrectly the FortiGate-5001E will not start up. Make sure the handles are correctly aligned, fully inserted and locked.

All chassis: Firmware problem

If the FortiGate-5001E is receiving power and the handles are fully closed, and you have restarted the chassis and the FortiGate-5001E still does not start up, the problem could be with FortiOS. Connect to the FortiGate-5001E console and try cycling the power to the board. If the BIOS starts up, interrupt the BIOS startup and install a new firmware image.

If this does not solve the problem, contact Fortinet Technical Support.

FortiGate-5001E status LED is flashing during system operation

Normally, the FortiGate-5001E Status LED is off when the FortiGate-5001E is operating normally. If this LED starts flashing while the board is operating, a fault condition may exist. At the same time the FortiGate-5001E may stop processing traffic.

To resolve the problem you can try removing and reinserting the FortiGate-5001E in the chassis slot. Reloading the firmware may also help.

If this does not solve the problem there may have been a hardware failure or other problem. Contact Fortinet Technical Support for assistance.

Fabric backplane communication speed compatibility

To make sure the FortiGate-5001E can successfully communicate with the fabric backplane you should make sure the fabric backplane interfaces are set to the correct speed for the chassis and the backplane switching device.

Do not set the FortiGate-5001E fabric backplane interfaces to auto negotiate. In most cases this setting will cause interruptions or compatibility issues.

This applies to fabric backplane interfaces fabric1 and fabric2 as well as any VLANs added to these interfaces. For example, SLBC configurations include interfaces such as elbc-ctrl/1 and elbc-ctrl/2 that must be able to connect to the fabric backplane.

For example, if the FortiGate-5001E is installed in a FortiGate-5144C chassis with a 40-Gbyte backplane the FortiGate-5001E fabric backplane interfaces should be set to 40000full:

```
config system interface
   edit fabric1
      set speed 40000full
   next
   edit fabric2
      set speed 40000full
   next
   edit elbc-ctrl/1
      set speed 40000full
   next
   edit elbc-ctrl/2
      set speed 40000full
   end
```

If the FortiGate-5001E is installed in a chassis with a 10-gbyte backplane (such as the FortiGate-5060 or 5140B) the FortiGate-5001E fabric backplane interfaces should be set to 10000full:

```
config system interface
   edit fabric1
      set speed 10000full
   next
   edit fabric2
      set speed 10000full
   next
   edit elbc-ctrl/1
      set speed 10000full
   next
   edit elbc-ctrl/2
      set speed 10000full
   end
```

FortiGate-5001E quick configuration guide

This section is a quick start guide to connecting and configuring a FortiGate-5001E security system for your network.

Before using this chapter, your FortiGate-5000 series or compatible ATCA chassis should be mounted and connected to your power system. In addition, your FortiGate-5001E should be inserted into the chassis and QSFP+ or SFP+ transceivers should be installed. The FortiGate-5001E should also be powered up and the front panel LEDs should indicate that the board is functioning normally.

Registering your FortiGate-5001E

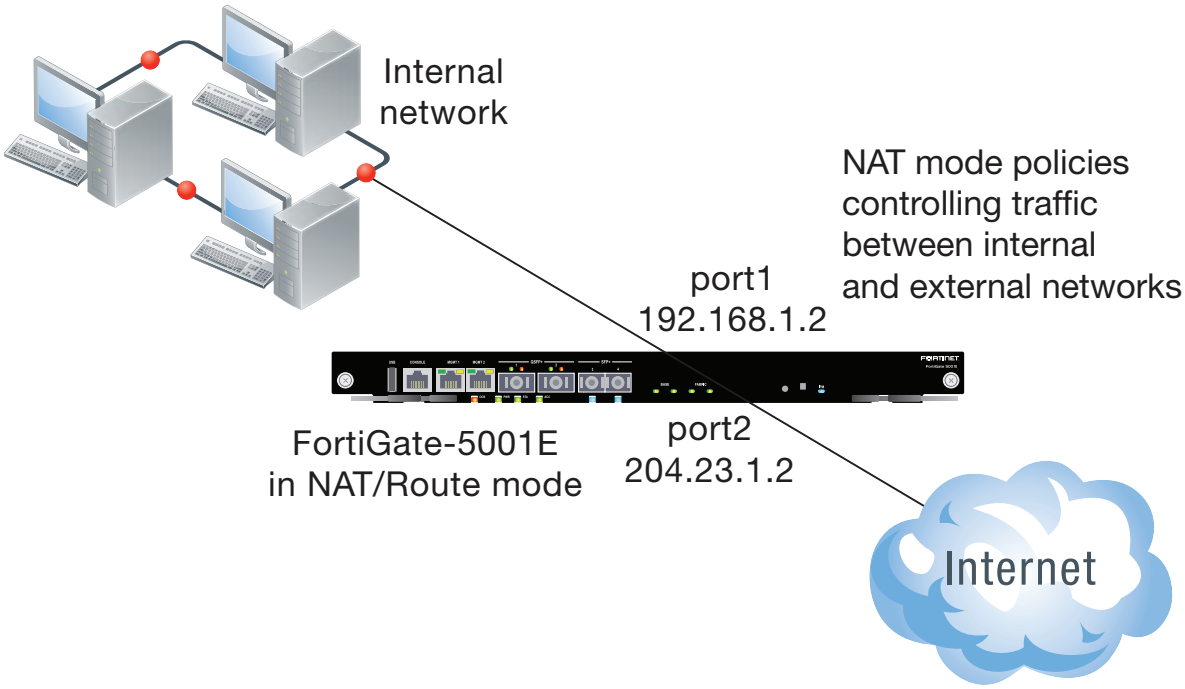
Register your FortiGate-5001E to receive Fortinet customer services such as product updates and customer support. You must also register your product for FortiGuard services. Register your product by visiting https://support.fortinet.com. To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased.

Planning the configuration

Before beginning to configure your FortiGate-5001E security system, you need to plan how to integrate the cluster into your network. In NAT/Route mode, the FortiGate-5001E security system is visible to the networks that it is connected to. Each interface connected to a network must be configured with an IP address that is valid for that network. In many configurations, in NAT/Route mode all of the FortiGate interfaces are on different networks, and each network is on a separate subnet.

You would typically use NAT/Route mode when the FortiGate-5001E security system is deployed as a gateway between private and public networks. In the default NAT/Route mode configuration, the FortiGate-5001E security system functions as a firewall. Firewall policies control communications through the FortiGate-5001E security system. No traffic can pass through the FortiGate-5001E security system until you add firewall policies.

In NAT/Route mode, firewall policies can operate in NAT mode or in Route mode. In NAT mode, the firewall performs network address translation before IP packets are sent to the destination network. In Route mode, no translation takes place.



Choosing the configuration tool

You can use either the GUI or the Command Line Interface (CLI) to configure the FortiGate-5001E. Some basic configuration settings can only be done from the CLI. You can connect to the GUI by connecting to mgmt1 using HTTP or HTTPS. You can connect to the CLI by connecting to mgmt1 using SSH or Telent or by a direct console connection to the FortiGate-5001E Console port. Use a terminal emulator with the following settings to connect to the console port: bits per second: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

Factory default settings

The FortiGate-5001E ships with the following factory default configuration.

Option	Default Configuration
Administrator Account User Name	admin
Password	(none)
mgmt1 IP/Netmask	192.168.1.99/24
mgmt2 IP/Netmask	192.168.100.99/24
Default route Gateway	192.168.100.1
Device	mgmt2

At any time during the configuration process, if you run into problems, you can reset the FortiGate-5001E to the factory defaults and start over. From the CLI enter `execute factoryreset`.

Basic GUI configuration

Use the following steps to set up a basic configuration.

1. Connect to the FortiGate-5001E mgmt1 interface by browsing to https://192.168.1.99.
2. Type **admin** in the **Name** field and select **Login**.
3. Change the admin administrator password by going to **System > Administrators**.
4. Edit the **admin** administrator and select **Change Password** to add a pasword.
5. To configure interfaces go to **Network > Interfaces** and edit each interface to configure.
6. To configure DNS setting go to **Network > DNS**.
7. To configure the Default Gateway go to **Network > Static Routes** and **Edit** the static route with destination 0.0.0.0/0.

Basic CLI configuration

Use the following steps to set up a basic configuration.

Use the serial cable supplied with your FortiGate-5001E to connect the FortiGate-5001E Console port or use SSH to connect to the mgmt1 interface CLI.

At the Login: prompt, type admin and press Enter twice (no password required).

Change the administrator password.

```
config system admin
   edit admin
      set password <password>
   end
```

Configure the mgmt1, port1, and port1 interfaces.

```
config system interface
   edit mgmt1
      set ip <intf_ip>/<netmask_ip>
   next
   edit port1
      set ip <intf_ip>/<netmask_ip>
   next
   edit port2
      set ip <intf_ip>/<netmask_ip>
   end
```

Configure the primary and secondary DNS server IP addresses..

```
config system dns
   set primary <dns-server_ip>
   set secondary <dns-server_ip>
end
```

Configure the default gateway.

```
config router static
```

```
edit 1
   set device <interface_name>
   set gateway <gateway_ip>
end
```

Upgrading FortiGate-5001E firmware

Fortinet periodically updates the FortiGate-5001E FortiOS firmware to include enhancements and address issues. After you have registered your FortiGate-5001E security system you can download FortiGate-5001E firmware from the support web site https://support.fortinet.com.

Only FortiGate-5001E administrators (whose access profiles contain system read and write privileges) and the FortiGate-5001E admin user can change the FortiGate-5001E firmware.

1. Copy the firmware image file to your management computer.
2. Log into the GUI as the admin administrator.
3. From the **System Information** widget, select **Update** beside **Firmware Version**.
4. **Select Upload Firmware**, select thefirmware image file that you downloaded. The FortiGate-5001E uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate-5001E login. This process takes a few minutes.
5. Log into the GUI.
6. Check the **Firmware Version** on the **System Information** widget to confirm the firmware upgrade is successfully installed.
7. Update the FortiGate-5001E antivirus and attack definitions.

FortiGate-5001E fabric and base backplane communication

By default the fabric and base backplane interfaces are not enabled. Once they are enabled you can operate and configure them in the same way as any FortiGate-5001E interfaces. Normally the fabric interfaces are used for data communication and the base interfaces are used for FGCP HA heartbeat communication. Although not recommended, you can use base backplane interfaces for data and HA heartbeat communication at the same time.

FortiGate-5001E fabric and base backplane communication requires a FortiSwitch or FortiController in switch mode installed in chassis slots 1 or 2. A FortiSwitch or FortiController in chassis slot 1 provides fabric communication on the fabric1 interface and base communication on the base1 interface. A FortiSwitch or FortiController installed in chassis slot 2 provides communication on the fabric2 and base2 interfaces.

Enter the following command to enable backplane data communication:

```
config system global
   set show-backplane-intf enable
end
```

The fabric1, fabric2, base1 and base2 interfaces now appear in all Interface lists. You can now configure the base backplane interfaces and add routes, firewall policies and other configuration settings using these interfaces.

On some chassis and with some hardware you may also have to change the fabric backplane interface speeds. Use the following command to do this:

To set the speed to be compatible with a 40-gbyte backplane:

```
config system interface
   edit fabric1
      set speed 40000full
   next
   edit fabric2
      set speed 40000full
   end
```

To set the speed to be compatible with a 10-gbyte backplane:

```
config system interface
   edit fabric1
      set speed 10000full
   next
   edit fabric2
      set speed 10000full
   end
```

Cautions and Warnings

Environmental Specifications

Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

Instructions de montage en rack - Les instructions de montage en rack suivantes ou similaires sont incluses avec les instructions d'installation:

Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Température ambiante élevée – S'il est installé dans un rack fermé ou à unités multiples, la température ambiante de fonctionnement de l'environnement du rack peut être supérieure à la température ambiante de la pièce. Par conséquent, il est important d'installer le matériel dans un environnement respectant la température ambiante maximale (Tma) stipulée par le fabricant.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Ventilation réduite – Installation de l'équipement dans un rack doit être telle que la quantité de flux d'air nécessaire au bon fonctionnement de l'équipement n'est pas compromise.

Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Chargement Mécanique – Montage de l'équipement dans le rack doit être telle qu'une situation dangereuse n'est pas lié à un chargement mécanique inégal.

Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Surtension – Il convient de prendre l'ensemble des précautions nécessaires lors du branchement de l'équipement au circuit d'alimentation et être particulièrement attentif aux effets de la suralimentation sur le dispositif assurant une protection contre les courts-circuits et le câblage. Ainsi, il est recommandé de tenir compte du numéro d'identification de l'équipement.

Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Fiabilité de la mise à la terre – Fiabilité de la mise à la terre de l'équipement monté en rack doit être maintenue. Une attention particulière devrait être accordée aux connexions d'alimentation autres que les connexions directes au circuit de dérivation (par exemple de l'utilisation de bandes de puissance).

Blade Carriers, Cards and Modems must be Listed Accessories or Switch, Processor, Carrier and similar blades or cards should be UL Listed or Equivalent.

Serveur-blades, cartes et modems doivent être des accessoires listés ou commutateurs, processeurs, serveurs et similaire blades ou cartes doivent être listé UL ou équivalent.

Refer to specific Product Model Data Sheet for Environmental Specifications (Operating Temperature, Storage Temperature, Humidity, and Altitude).

Référez à la Fiche Technique de ce produit pour les caractéristiques environnementales (Température de fonctionnement, température de stockage, humidité et l'altitude).

Safety

Moving parts — Hazardous moving parts. Keep away from moving fan blades.
Pièces mobiles – Pièces mobiles dangereuses. Se tenir éloigné des lames mobiles du ventilateur.

Warning: Equipment intended for installation in Restricted Access Location.
Avertissement: Le matériel est conçu pour être installé dans un endroit où l'accès est restreint.

Warning: A readily accessible disconnect device shall be incorporated in the building installation wiring.
Avertissement: Un dispositif de déconnexion facilement accessible doit être incorporé dans l'installation électrique du bâtiment.

Battery – Risk of explosion if the battery is replaced by an incorrect type. Do not dispose of batteries in a fire. They may explode. Dispose of used batteries according to your local regulations. IMPORTANT: Switzerland: Annex 4.10 of SR814.013 applies to batteries.

Batterie – Risque d'explosion si la batterie est remplacée par un type incorrect. Ne jetez pas les batteries au feu. Ils peuvent exploser. Jetez les piles usagées conformément aux réglementations locales. IMPORTANT: Suisse: l'annexe 4.10 de SR814.013 s'appliquent aux batteries.

警告
本電池如果更換不正確會有爆炸的危險
請依製造商說明書處理用過之電池

Caution: Disconnect power supply cords before servicing

Attention: Débranchez les cordons de la source d'alimentation avant tout entretien.

Grounding — To prevent damage to your equipment, connections that enter from outside the building should pass through a lightning / surge protector, and be properly grounded. Use an electrostatic discharge workstation

(ESD) and/or wear an anti-static wrist strap while you work. In addition to the grounding terminal of the plug, on the back panel, there is another, separate terminal for earthing.

Mise à la terre — Pour éviter d'endommager votre matériel, assurez-vous que les branchements qui entrent à partir de l'extérieur du bâtiment passent par un parafoudre / parasurtenseur et sont correctement mis à la terre. Utilisez un poste de travail de décharge électrostatique (ESD) et / ou portez un bracelet anti-statique lorsque vous travaillez. Ce produit possède une borne de mise à la terre qui est prévu à l'arrière du produit, à ceci s'ajoute la mise à la terre de la prise.

This product has a separate protective earthing terminal provided on the back of the product in addition to the grounding terminal of the attachment plug. This separate protective earthing terminal must be permanently connected to earth with a green with yellow stripe conductor minimum size # 6 AWG and the connection is to be installed by a qualified service personnel.

Ce produit a une borne de mise à la terre séparé sur le dos de l'appareil, en plus de la borne de mise à la terre de la fiche de raccordement. Cette borne de mise à la terre séparée doit être connecté en permanence à la terre avec un conducteur vert avec la taille bande jaune de minimum # 6 AWG et la connexion doit être installé par un personnel qualifié.

Caution: Slide/rail mounted equipment is not to be used as a shelf or a work space.

Attention: Un équipement monté sur bâti ne doit pas être utilisé sur une étagère ou dans un espace de travail.

Fiber optic transceiver must be rated 3.3V, 22mA max, Laser Class 1, UL certified component.
Le transceiver optique doit avoir les valeurs nominales de 3.3 V, maximum 22 mA, Laser Class 1, homologué UL.

Regulatory Notices

Federal Communication Commission (FCC) – USA

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received; including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

WARNING: Any changes or modifications to this product not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Equipment Standard for Digital Equipment (ICES) – Canada

CAN ICES-3 (A) / NMB-3 (A)

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Cet appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicte par le ministère des Communications du Canada.

European Conformity (CE) - EU

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Voluntary Control Council for Interference (VCCI) – Japan

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。VCCI－A

Product Safety Electrical Appliance & Material (PSE) – Japan

日本では電気用品安全法(PSE)の規定により、同梱している電源コードは本製品の専用電源コードとして利用し、他の製品に使用しないでください。

Bureau of Standards Metrology and Inspection (BSMI) – Taiwan

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

China

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。这种情况下，可能需要用户对其采取切实可行的措施。